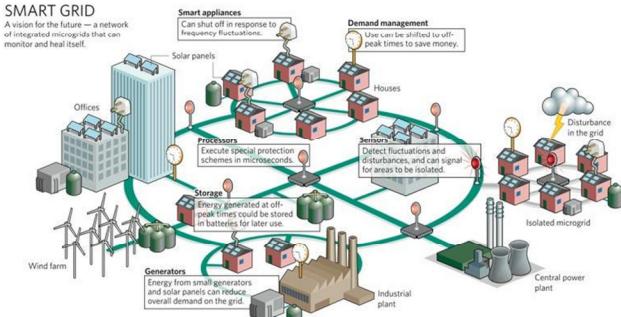


An Introduction - Smart Grid 101

Chapter 9: Privacy



Chuck Goldman, Project Manager
Electricity Markets and Policy Group
Lawrence Berkeley National Laboratory

Deirdre K. Mulligan
Assistant Professor, School of Information
and Director, Berkeley Center for Law and
Technology

Jennifer M. Urban
Assistant Professor of Law and
Director of the Samuelson Law,
Technology & Public Policy Clinic

June 2011

University of California Berkeley Boalt Hall School of Law

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

The Smart Grid is a compilation of concepts, technologies, and operating practices intended to bring the electric grid into the 21st century. Smart Grid concepts and issues are difficult to address because they include every aspect of electric generation, distribution, and use.

While the scope of smart grid covers the entire utility system from generation to how customers use energy, this chapter addresses the topic of demand response.

Our objective throughout this chapter is to more clearly define demand response, to point out policy, technology, and customer behavior combine to define the capabilities and potential benefits of Smart Grid.

***Note:**

The original slides were developed for a Webinar delivered on June 10, 2011. Much of the material in the June Webinar was based on a Proposed Decision from the California Public Utilities Commission (CPUC), which was considered the first, comprehensive regulatory decision to address smart grid privacy issues.

On July 29, 2010 the CPUC issues a Final Decision to close out their Privacy Proceeding. The notes to this slide deck have been updated to reflect the final decision. The Final Decision made substantial changes in the CPUC jurisdiction over customer data and privacy.

The organizers consider the differences between the Proposed and Final Decisions significant, consequently in many cases the notes to these slides present both interpretations. Proposed decision notes are presented in 'normal' black colored font. Final Decision changes are presented in "blue" colored font.

Contents



Section	Topic	Slides
1	Information Privacy	3-4
2	Smart Grid	
	▪ New Information Flows	5-10
	▪ New Entities	11-12
	▪ Gaps in Legal Regulatory Frameworks	13-19
3	CPUC Decision	20-37
4	References	38
5	Contact Information	39

8/30/2011

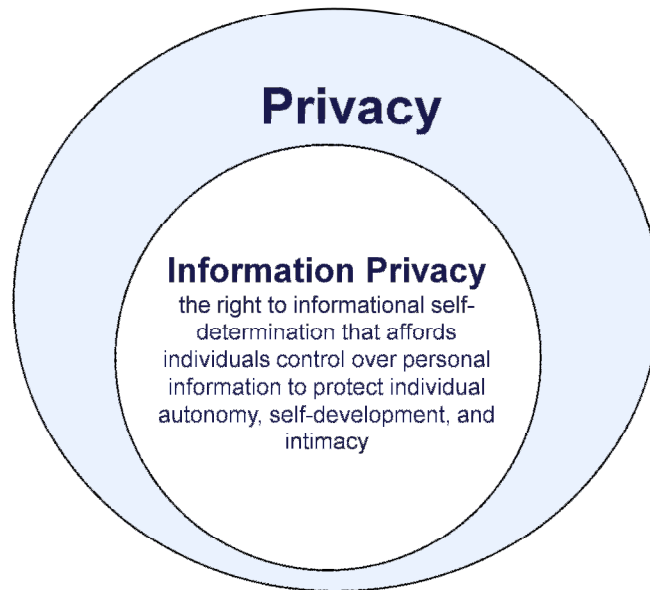
Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

2

The contents of this chapter are divided into six sections.

- As with our prior webinars and chapters, we start with a narrow set of objectives and try to focus on attention on demand response (DR) issues principally related to regulatory policy.
- Section 4 provides updated information on the two principal NIST standards efforts related to DR.

Definition of Privacy



8/30/2011

Lawrence: Bezdek's Hologram Laboratory - Smart Grid Technical Advisory Project

3

What is privacy. Is it really an ambiguous concept or can a more narrow definition be established.

For this webinar we are focusing on information privacy. It is a well defined concept that is specified in this definition. The primary context of information privacy is to provide individuals with control over personal information. This definition is well established both in the US and other parts of the world.

Fair Information Practices (FIP) Principles



- §2. Transparency** – organizations should provide notice to individuals regarding their use, disclosure, and retention of personally identifiable information (PII).
- §3. Purpose Specification** – organizations should seek individual consent to collect, disclose, and retain PII.
- §4. Individual Participation** – organizations should articulate specific purposes for collecting PII, and specific uses for PII they collect.
- §5. Data Minimization** – organizations should collect only PII that is “directly relevant and necessary to accomplish the specified purpose(s)” and retain data no longer than necessary.
- §6. Use & Disclosure Limitation** organizations should use PII only for the purposes stated in their notices.
- §7. Data Quality & Integrity** organizations should keep PII accurate, relevant, timely, and complete.
- §8. Data Security** – organizations should implement adequate safeguards to protect against loss, unauthorized use, modification, and unintended disclosure.
- §9. Accountability & Auditing** – organizations should audit employees’ and contractors’ actual use of PII, to ensure compliance with the other FIPs.

8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

4

This definition of privacy has been operationalized and implemented through a set of what is referred to as Fair Information Practices (FIP) and Principles.

The eight principles provided on this slide is only one version of FIPs that have been developed to address multiple sectors that go back to one of the original developments by the Department of Health Education and Welfare in the 1970's. At the international level FIPs are recognized by the Organization for Economic Cooperation and Development and in the European Union by State of Protection Directives.

In the US many statutes refer to and reflect these principles. These FIPs are also referred to in the NIST security and privacy working group documents as well as the CPUC privacy decision.

Information Flows



- ❑ **Source of Data**
- ❑ **Recipient**
- ❑ **Use**
- ❑ **Mechanism of transmission**
- ❑ **Nature of the data (explicit and implicit)**

8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

5

Many of the slides that follow will concentrate on information flows, especially the new sources of data and devices that are expected to be introduced by the smart grid.

The smart grid may be viewed as an early instantiation of the Internet of 'things' where devices within the customer home will be individual addressable and designed to provide data and interact within the home and utility network.

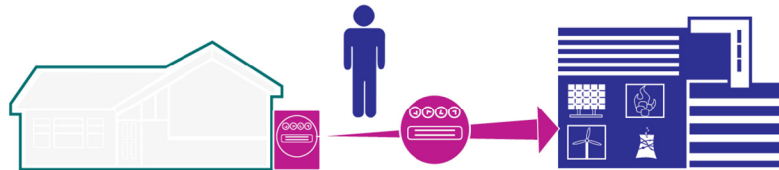
There will be new recipients of this data that go beyond the utility.

Uses of information will provide opportunities to make more and better uses of this data. However, there are also many other uses that may impact privacy.

Networking the home and grid will also impact the movement of data.

Finally, the nature of data is important. What can the data tell us at a meta level regarding energy use at a community as well as at the micro level regarding what this data can tell us for an individual customer or premise.

Electromechanical meter to utility



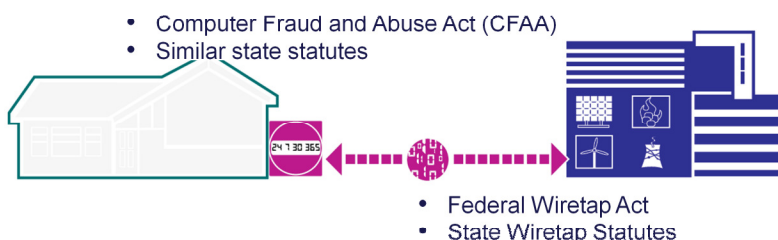
This graphic reflects the old world, where electro-mechanical meters require a person to physically visit (or come within close approximation) of each utility customer premise to read and then transmit meter readings back up to the utility.

Information Flows



Smart Meter to Utility Protections against unauthorized access

- Computer Fraud and Abuse Act (CFAA)
- Similar state statutes
- State specific utility statutes and regulations
- State Security Breach Notification Statutes



8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

7

Protections against unauthorized access.

In the new smart grid world, meters include technology embedded with computing and communication capability that enables the collection, tracking, and periodic transmission of data back to the utility.

There are a host of protections to address authorized and unauthorized access, both of which may raise privacy concerns. There are a host of state statutes and federal rules that already address privacy and security in the utility space regarding unauthorized access. At the meter, the Computer Fraud and Abuse Act and similar state statutes that make it a criminal offense for people to access the information within those devices without authorization or to exceed authorization. Regarding the flow of information from the meter to the utility there are protections provided through the Federal Wiretap Act and state equivalents which make it a criminal offense to intercept data during the flow.

Finally back at the utility, protections are enabled by the Fraud and Abuse Act and similar state statutes. There are also individual state public utility acts that come into play. There are also notification statutes that create triggering events that require utility notify customers of breach events. In some cases encrypted information may be exempt from these notification statutes, which in an indirect way encourages companies that maintain customer account and other data to engage in data encryption and other security practices.

Smart Meter to Utility Rules constraining lawful access

- State statutes
- State constitutions



9/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

8

Rules Constraining Lawful Access.

One concern is regulatory gaps that may not sufficiently constrain illegal or unauthorized access to data. We are also concerned about situations that create a lack of parity due to the entrance of new players into the smart grid with respect to statutes and constitutional provisions that limit lawful access to data.

Lawful access to data includes: (a) what are the procedural standards that regulate how data can be obtained, does it require court action, do you need to issue a subpoena, and (b) substantive standards that consider relevance or is it provided under a clear and convincing evidentiary finding for law enforcement access to information. In addition what are the standards for third-party civil litigants or new business partners which may want to share information.

For utilities there are state statutes and public utility rules that govern how utilities store, use, and disclose data. These also frequently address how law enforcement gain access to data from public utilities.

Many states have constitutional provision may provide a framework or may be interpreted to define specific rules for law enforcement access. These frameworks at the state level may or may not define the rules for third-party access to this data. Public utility rules that govern the extent to which utilities can disclose specific data about a particular account versus aggregate accounts are all rules that constrain lawful access, not unlawful access..

Information Flows

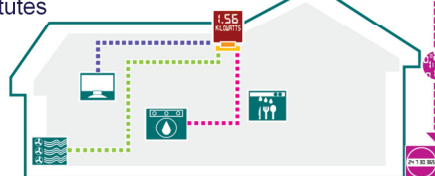


Customer-owned Meter

- Computer Fraud and Abuse Act (CFAA)
- Similar state statutes
- State specific utility statutes and regulations
- State security breach notification statutes



- Computer Fraud and Abuse Act (CFAA)
- Similar state statutes



Federal Wiretap Act
State Wiretap Statutes

A customer-owned meter (shown at top of house), separate from the utility-owned smart meter, gathers usage data and sends it to internal home network devices. The data does not leave the house.

8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

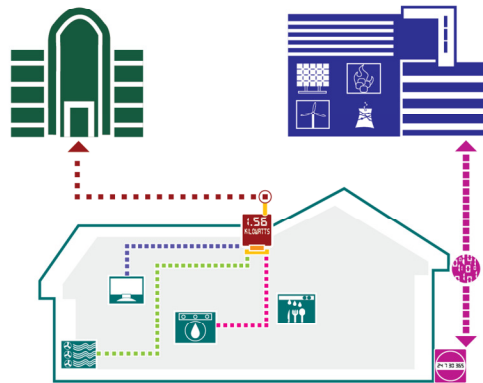
9

Customer Owned Meter

One of the new things being introduced by smart grid is the customer owned meter, in addition to the utility owned meter. The term customer owned meter is being used here in a general sense. This term could include something like a “TED” device that is wired into the customer service panel to provide access to information wirelessly to other customer owned devices. The same set of legal and illegal access statutes apply here. However, now we have data and identifiers relevant to specific devices, where in this case that information stay in the home. The flows of data within the home are covered by the Federal Wiretap Act . Retaining this information in the home means this information does not become a business record of a third-party which also means this information is still protected under the 4th Amendment protections.

Security of this information is also dependent upon whether this information is moved over a wired network or a wireless network restricted to operate only within the home. Wireless movement of this data over a public network may reduce privacy protections.

Customer-owned Meter



A customer-owned meter (shown at top of house), separate from the utility-owned smart meter, sends usage data to a third party.

8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

10

Customer Owned Meter

In this data flow there is a separate customer owned meter where the data flows out to a third-party, not to the utility. The next few slides will cover three different configurations or ways in which this customer owned meter data can flow between specific parties, each with slightly different legal and regulatory concerns.

Information Flows



Customer-authorized third party access to data from utility



No personal meter — e.g. Google gets customer data from utility based on customer authorization.

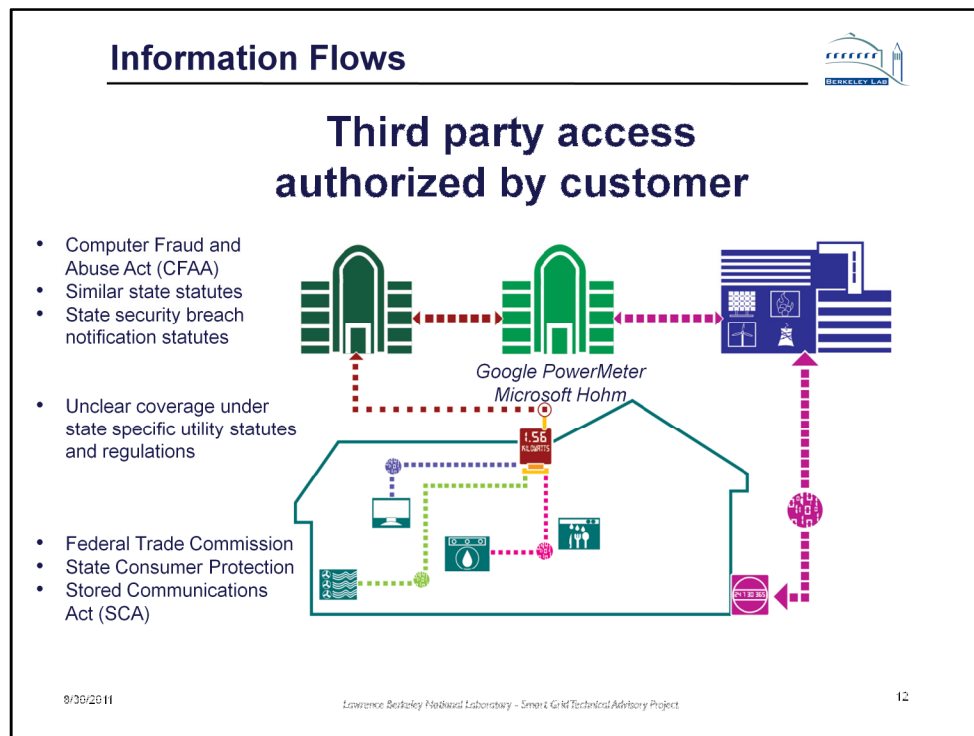
8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

11

Customer Authorized Third-Party access to utility data.

In this example there is no separate customer meter however there is an internal home area network. Customer usage data flows to the utility and independently the customer has authorized or provided permission to a third-party to access their data directly from the utility data.



Third party access authorized by the customer.

In this example the customer authorizes third-party access, however the data is coming both from the home through a separate metering infrastructure and from the utility.

In all of these options, the Computer Fraud and Abuse Act and similar state statutes to the extent we are dealing with third-party entrance into the smart grid are covered by state security breach statutes. The extent to which these third-party entities are covered under state specific utility statutes that provide privacy protections is unclear and will have to be decided on a state-by-state basis.

Information flowing within the home that flows out of the home either through the customer owned meter or through the utility to third-party entities, there are state consumer protection laws and also potential protections that may be provided by the Federal Trade Commission. The FTC is looking at privacy protections and beginning to establish rules that obligates a standard of care. This may include putting programs in place to attend to security risks, stay updated on vulnerabilities, and provide mitigation.

Finally, the Stored Communications Act (Federal) provides protections for access both against unauthorized access and authorized access to data stored in third-party sites.

Home Area Network (HAN)



☐ Privacy and Innovation

- Tracking and Monitoring
- Registration
- Demand Response and Load Control
- Pricing, Messaging, and Billing Information


8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

13

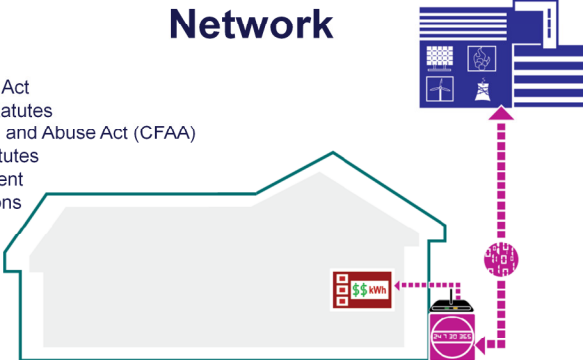
Home Area Network (HAN) – balancing privacy with innovation and competition

Home Area Network (HAN)



Real-time usage data in Home Area Network

- Federal Wiretap Act
- State Wiretap Statutes
- Computer Fraud and Abuse Act (CFAA)
- Similar state statutes
- Fourth Amendment
- State Constitutions



A HAN gateway (black device attached to the smart meter), sends energy usage information to an in-home display, which presents real-time energy consumption and price information to the customer.

8/30/2011
Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project
14

Home Area Networks (HAN)

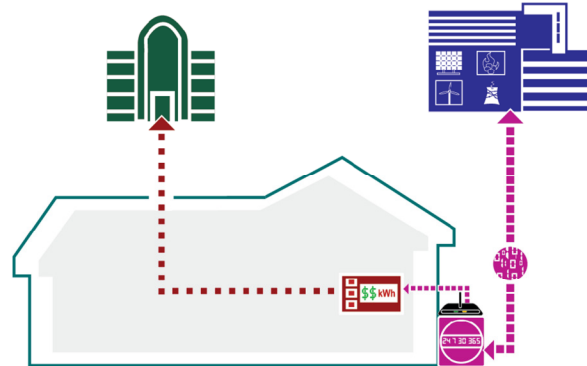
Tracking and Monitoring – the home is becoming populated by a number of smart devices that are interacting with a network. That network will use a gateway that acts to coordinate and manage these devices. Smart Meters may include a home area gateway designed and included in the meter. There is no reason why this gateway has to reside in the meter. The gateway is just an interface that is used to interface between the home devices and meter.

The gateway may provide the interface for managing price and other data passing to devices to regulate customer response. It may also be used to pass data from devices in the home back to the utility. Data that does not leave the home is covered by 4th Amendment protections against unauthorized access, however with data leaving the home and passing back to the utility the 4th Amendment has little relevance although these protections may change. There may be state constitutional protections to address this situation.

Home Area Network (HAN)



Data shared with a third party from HAN via home device



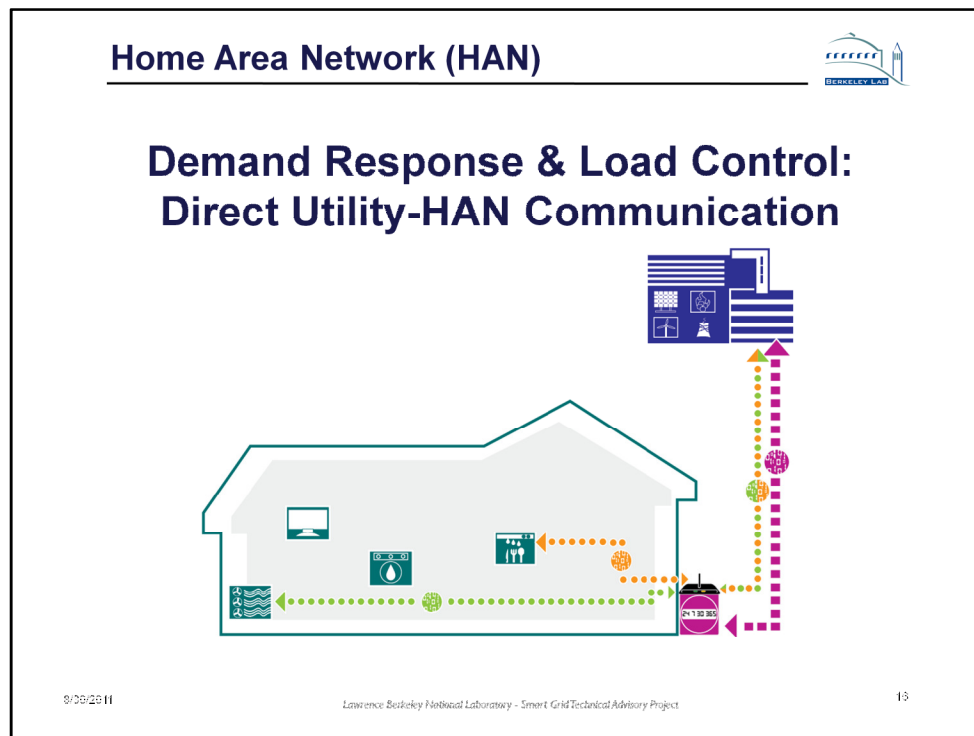
8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

15

Home Area Networks (HAN)

Data Shared with a Third Party from a HAN - see slide #12.



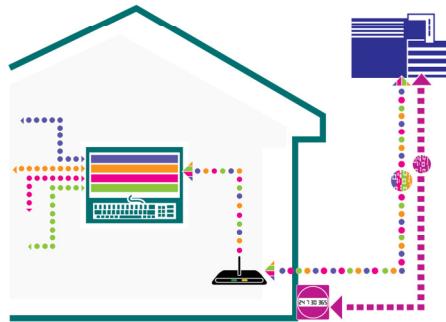
Home Area Networks (HAN)

Demand Response & Load Control: Direct Utility HAN Communication.

In this scenario the utility provides load control or pricing signals to the home through the meter, which passes this information to the HAN gateway to the customer energy management system/devices which control those devices based on customer decisions.

One option would be to provide a technical barrier around the home where all information about how the customer and devices respond is kept within the home. The decision regarding how the customer responds is shared with the utility based on meter data usage information, not specific information regarding particular premise devices.

Customer-owned Energy Management System



8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

17

Demand Response & Load Control:

Customer Owned Energy Management System

In this scenario a customer owned energy management system provides protection by shielding the devices and individual decisions from the interface with the meter.

Demand Response & Load Control



Third-party Energy Management System



8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

18

Demand Response & Load Control

Third-Party Energy Management System.

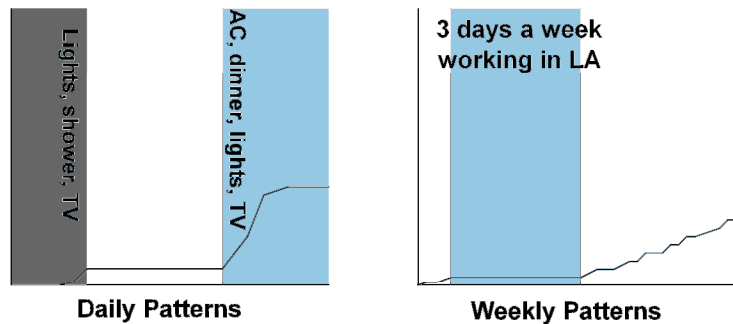
In this scenario the utility is sending load control and pricing information into the home. The utility meter is sending back some information in the home back to the utility on usage, however no customer device or specific decision information is provided back to the utility.

Where the customer uses a third-party energy management system, it may be sending information back to the third-party provider.

Interval Data



- 3000 data points per month for 15-minute intervals – vs. 1
- Virtual biography of household activity in near real-time
- Adding specific appliance data (e.g., smart dryers, PEVs) adds even more detail



Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

Why are these various data flow scenarios important? The data being collected with smart meters is much more detailed than what was possible with once a month meter reads. The more detailed data make it much easier to identify the patterns of usage – which appliances are using data and when they are using energy. Under some scenarios, customers will have to register their appliances to qualify for certain demand response programs which may then enable the utility to not only know exactly what appliances they have but will also allow the utility to retrieve certain detailed settings and operating statistics for those appliances.

The basic point is that this data is not the same as it was before. 1 point of data a month for the whole house is of a totally different character than is 3000 points (every 15 minutes), especially when additional appliance specific data may also be collected. More can be learned or inferred about the inhabitants of the home - when are they home, what are their occupancy patterns - this may be of interest to a variety of audiences, specifically:

- Marketers - may wish to buy data and sell it to other product and service providers
- Criminals - can determine homes that have occupancy patterns making them easy to rob - data mining for targets
- Abusers/etc - may be able to determine activities remotely to target their harassment or collect information with adverse legal or financial implications.

There is also an issue or set of questions that need to be raised regarding innovation and the ownership and control of the customer energy management system(s) and the HAN gateway. If you have Internet access, consider your experience with your service provider. Your Internet Service Provider does not tell you what router you can have in your home, nor do they tell you which devices may interact with your router. This approach enhances privacy and it also encourages innovation among product and service providers. These practices are supported by open standards establish how these devices connect, provide security and privacy, and allow for innovation in the development of products and services. With the utility in control of the HAN gateway we have to question whether the regulators and utility can support the innovation necessary to support customer needs and whether they can devote the resources (technical and financial) to continually update and provide reasonable levels of security and privacy.

CPUC Proposed Decision May, 2011

8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

20

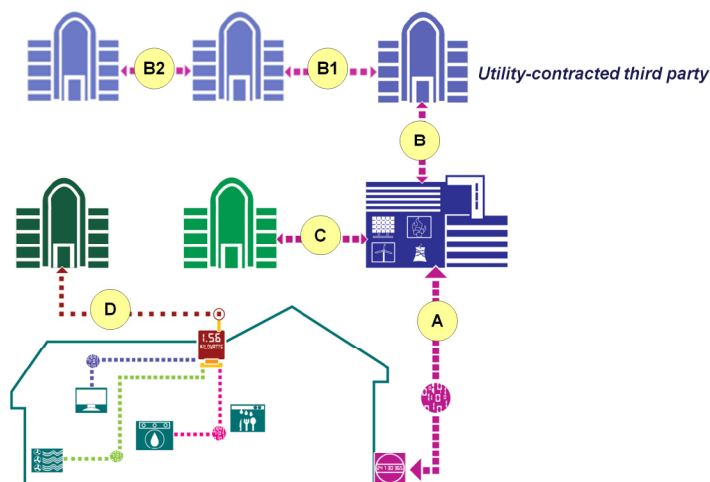
As one of the first regulatory decisions to address Smart Grid privacy, we want to use the CPUC Proposed Decision as a framework to address many of the key issues.

State legislation (SB17) required that the CPUC address a host of regulations around the smart grid. Privacy issues related to smart meters was just one of the elements they were required to address. To address privacy, the CPUC held public workshops and solicited written comments from the participating parties.

As additional background it is important to point out that Professor Urban's clinic represented the Center for Democracy and Technology, a non-profit organization that focuses on consumer information privacy issues emanating from technological change. The Center for Democracy and Technology was an active participant in the CPUC Privacy proceeding.

The Center for Democracy and Technology together with the Electronic Frontier Foundation proposed a set of rules drawn from the Fair Information Practices (FIPs) that formed one basis for the rules adopted by the CPUC in their proposed decision.

Data Flows



8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

21

This is a simplified model of the data flows that California has been considering that are indicative of what every other state should anticipate.

Under this model, privacy rules need to look at several different data flows, specifically:

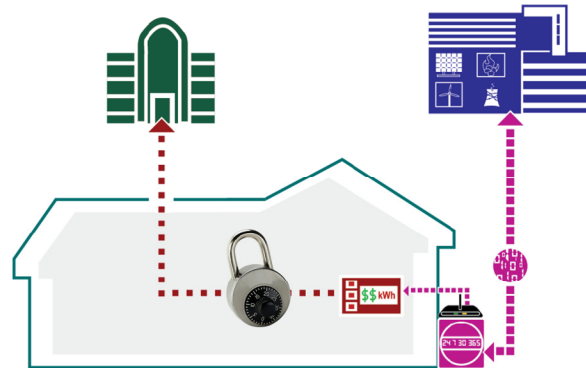
1. [A] from the utility-owned smart meter to the utility,
2. [B] from the smart meter to the utility and then from the utility to third-party providers that deliver services to the utility (*as its agent*) for billing, web site support, and other functions. These service providers may in turn pass the same customer data on to their service providers [B1] and [B2]
3. [C] data may also flow from the smart meter to the utility and then from the utility to third-party providers selected by the customers – like Google PowerMeter or Microsoft Hohm.
4. [D] finally, the customer may also provide data from consumer-owned devices within the home to other third-party service providers directly.

Each of these data flows have privacy implications and raise questions regarding which organization and which rules or laws govern.

CPUC Decision



Data shared with a third party from HAN via “locked” device



8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

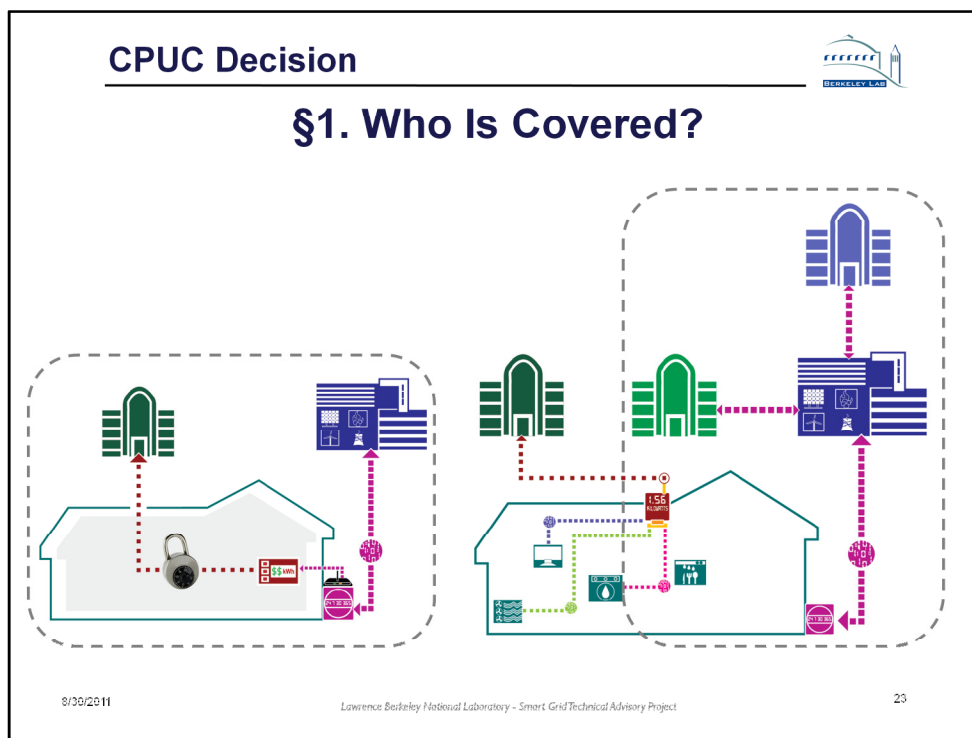
22

One of the key questions raised in the proceeding addressed what data is covered and which actors (participants) are covered by proposed rules within the CPUC draft decision?

The proposed decision singles out what they refer to as a ‘locked device’ that is registered to the utility HAN, that receives information from the smart meter through the HAN that then provides information to a third-party. The locked feature uses the analogy of the smart phone that is locked to a single service provider. The concept of a “locked device” was considered confusing by many interveners who raised many questions during the proceeding regarding the need for this distinction.

NOTE:

Although the Proposed Decision exercised CPUC regulatory jurisdiction over data that flows from a gateway within the smart meter to a device “locked” to a particular customer-selected third-party provider (similar to a cell phone being locked to a particular provider’s network), the Final Decision did away with the reference to and concept of “locked devices” entirely.



Principal #1: Who is covered by a regulation or rule?

The remainder of this presentation will step through the Fair Information Practice principles (FIPs) that the CPUC has incorporated into its proposed decision and try to illustrate how a regulatory commission can apply them to each of these data flows.

How far does the rule or principle extend? We've used the dashed rectangles above to illustrate for each of the two data flows, which parties would actually be subject to regulation.

For example, on the left example, the third-party that receives data from a locked device through the HAN, which the utility has to turn on, is included in the regulatory domain and would be subject to all regulatory conditions. [See slide #22. The "locked device" concept was removed from the Final Decision.](#)

In the diagram on the right, each of the parties that receive information under some contractual arrangement from the utility would be subject to the regulatory rules and regulations. Each contractual arrangement will include appropriate terms and conditions. In this data flow example, the third-party that receives information directly from a customer-owned devices, not through the HAN or utility meter, is not included in the regulatory domain.

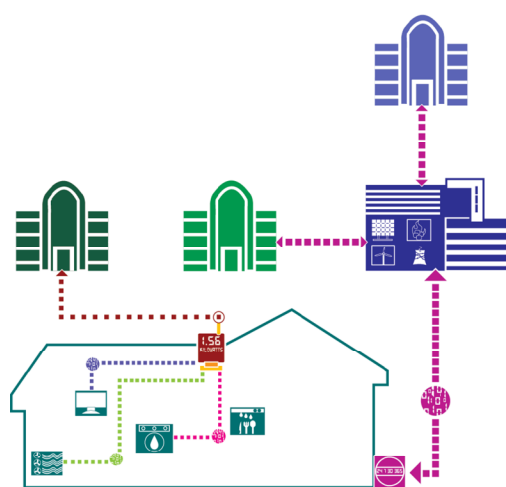
Final Decision Clarifications -Parties Covered by Privacy Regulations:

- Investor-owned utilities
- Utility contractors (agents of the utility) including contractors in support of energy efficiency, demand response, and other programs authorized by the Commission (Decision pg 29-30).
- The CPUC deferred jurisdictional questions regarding third-party contractors who receive data from utility backhaul or gateways in the meter on behalf of the customer.
 - Backhaul issues will be resolved during tariff proceedings , specifically whether it is reasonable to establish registration and standard practices for data usage (Decision pg. 31)
 - Smart Meter Gateway issues – not covered by the Final Decision.

CPUC Decision



§1. Definitions



(a): **Covered Entity:** electrical corporations and third parties who obtain information via the utility or a “locked” device.

((b) **Customer:** Recipient of retail generation, distribution or transmission service (ongoing discussion re “entity”).

(c): **Covered Information:** usage information obtained through AMI *if* it is associated with any information that can reasonably be used to identify a customer; does not cover information that cannot be reasonably identified or re-identified.

8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

24

Definitions: What is covered and who is protected by the rule?

What is the covered information? All privacy rules are specific to the types of data being collected and transported. The information covered by the rules includes all usage information collected through advanced metering but only if it is associated with identifying information that can be used to identify the customer or if the information can be re-identified. As long as the data is not connected to an individual, most of the privacy issues have been addressed, however if capability exists to re-identify the actual customer, then privacy becomes an issue. So the rules will cover data that has been determined to be in a reasonable stable state, that cannot be re-identified.

- “Covered Entity” no longer includes third parties who obtain data via a “locked” device
- “Covered Entity” now includes the third parties who receive data on order of the Commission (these third parties appear to be those working for the Commission, as described in the notes to Slide 23.
- The definition of “customer” was deleted as redundant, and is not included in the final rule. (It was also unclear, as noted on the slide, whether the Proposed Decision’s definition would cover individual customers.)


Important Note:

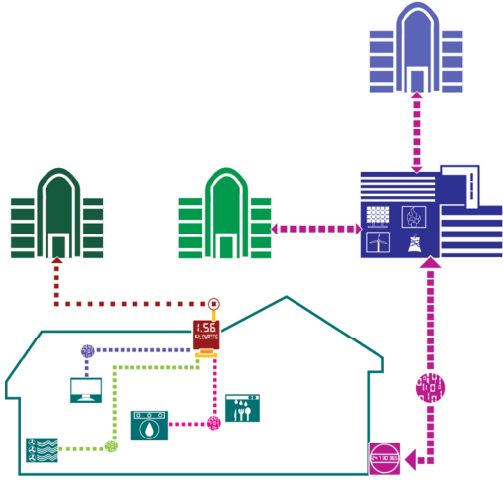
This slide mistakenly does not include the definition of **primary purpose** – it should. “Primary purposes” are defined to cover fundamental energy needs: to provide or bill for electrical power or gas; or to provide for system, grid, or operational needs. “Primary purposes” can also be providing legally required services, or those specifically authorized by Commission order; or for demand response, energy management, or energy efficiency programs under contract with a utility, under contract with the Commission, or as part of a Commission authorized program by a government entity under the Commission’s supervision. As such, third parties that do not fit into the foregoing categories *do not* engage in primary purposes—only secondary purposes.

This is important to understanding the rule, because only primary purposes may be undertaken without prior, opt-in consent by the customer. All other purposes require prior consent.

CPUC Decision

§2. Transparency





(a): Must provide customers with "clear, accurate, and specific notice regarding the collection, storage, use, and disclosure of covered information."

There are requirements for when notice must be provided and, notably, what must be included in the notice

8/30/2011
Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project
25

Principle #2: Transparency

The rules track the list of FIPs presented in Slide #4.

Transparency assumes that customers can make good choices if they have good information. If they don't have good information it is difficult to make meaningful choices.

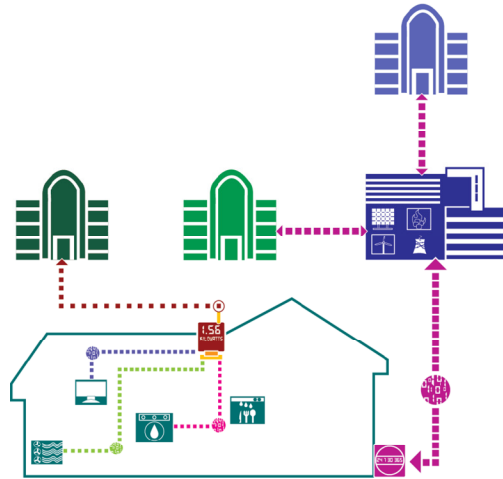
The key to the CPUC implementation of "transparency" is that it be genuine. The proposed decision addresses specific types of information individually. All information must be clear, accurate and specific. These requirements are important because privacy has always been dependent upon customer notice and choice. We give customers notice and they make a choice. However, notices can be particularly vague. The rule states that notices must be clear and makes specific recommendations to interpret the options.

The Final Decision clarifies that electronic forms of notice may be used.

§3. Purpose Specification

Must provide

- (a)(1): What categories of information are information stored and reasonably specific purposes for why it is stored
- (a)(2): What categories of information are provided to third parties and purpose; some information about third parties
- (b): How long information is retained
- (c) Information on means or dispute or minimization by customer



8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

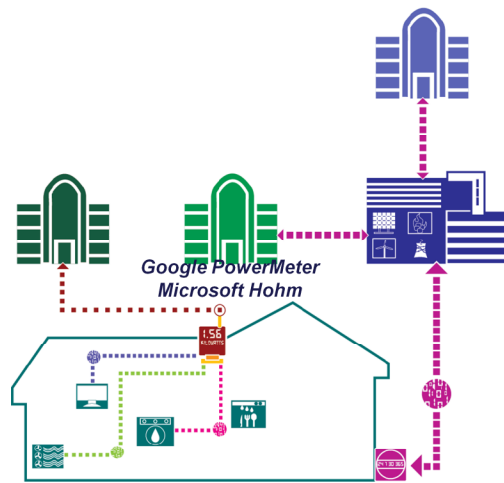
26

Principle #3: Purpose Specification

This goes along with notice. First the individual is told what information you intend to collect and then for what purpose is it being collected and stored and for what purpose might you disclose that information. The purpose specification rule requires that each category of information being collected be explained, how long the information will be collected, and ways in which customers can limit the collection and storage of that information.

This rule covers differently information disclosed for primary versus a secondary purpose. Information for a primary purpose is something related to the provision or operation of demand response or efficiency necessary to their primary business. Secondary purposes would include anything else, such as marketing to device manufacturers, for insurance sales, or for appliance maintenance issues.

§4. Individual Participation



(a) Customers have access to their covered information

(b)(1): Customers have the right to grant or revoke secondary uses of covered information, to dispute accuracy, and request corrections

(c) Rules for Legal Process

8/30/2011

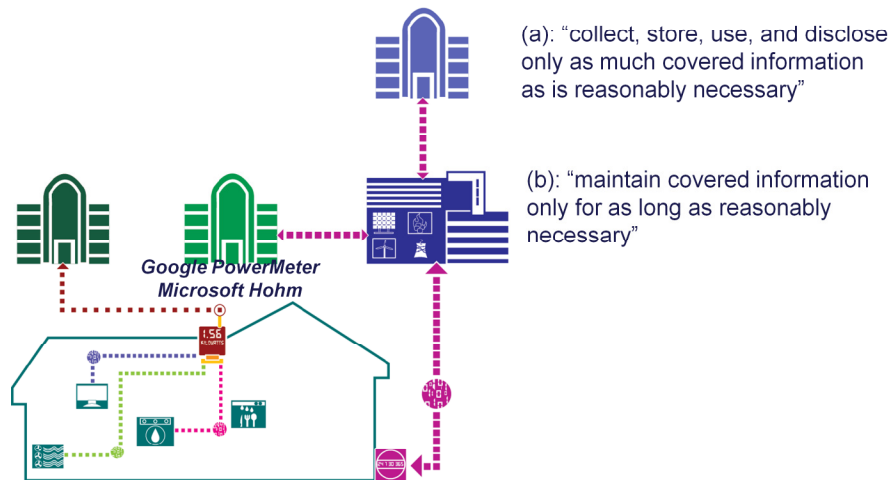
Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

27

Principle #4: Individual Participation

The person whose data is being disclosed or used must have the capability to participate in how it is being used. They must be given notice, the purpose must be described, they must exercise consent. Customer must also have access to their information in a easily readable format. This rule also describes the rules for legal process.

§5. Data Minimization



8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

28

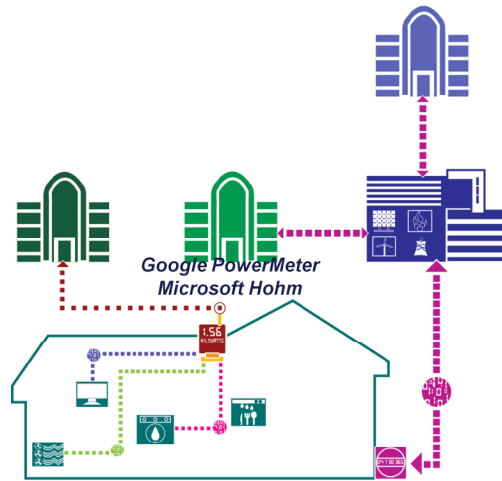
Principle #5: Data Minimization

When a company is planning a new business practice, data minimization under FIPs requires that they consider what data is minimally required to fulfill that purpose. This approach must justify what is necessary and how and for how long it is stored. Basically, minimizing data collection also limits any potential problems arising from breaches of stored data or operating systems.

CPUC Decision



§6. Use & Disclosure Limitation



(b): Utilities “may collect, store and use covered information for primary purposes without customer consent.”

(b): Third parties “may collect, store and use covered information only with prior customer consent. *Exception:* utilities may disclose info when ordered to do so by the Commission or for a primary purpose being carried by contract on behalf of the utility

8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

29

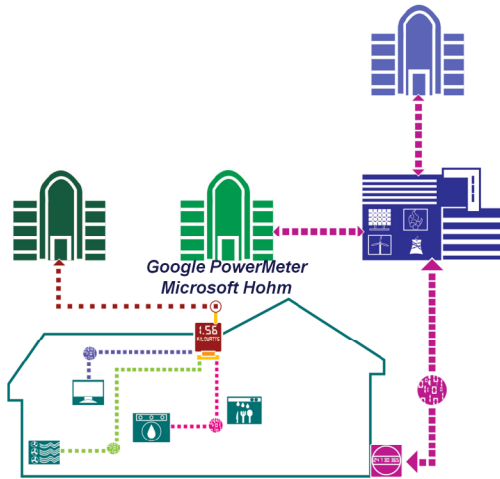
Principle #6: Use & Disclosure Limitation.

The heart of this rule focuses on whether the data is being used or disclosed for primary or secondary purposes. Utilities can collect and use primary data without customer consent because that data/information is essential to their basic business function. However, third-parties may not collect data without customer consent.

There is an exception to this rule as it applies to utilities when they disclose information when ordered to do so by the Commission or to a third-party under a utility contract whose purpose is to support a primary utility function.

As noted in the notes for slide 24, only certain entities engage in “primary purposes,” which may be undertaken without customer consent. These parties changed somewhat from the Proposed Decision—please see notes to slide 24.

§6. Use & Disclosure Limitation



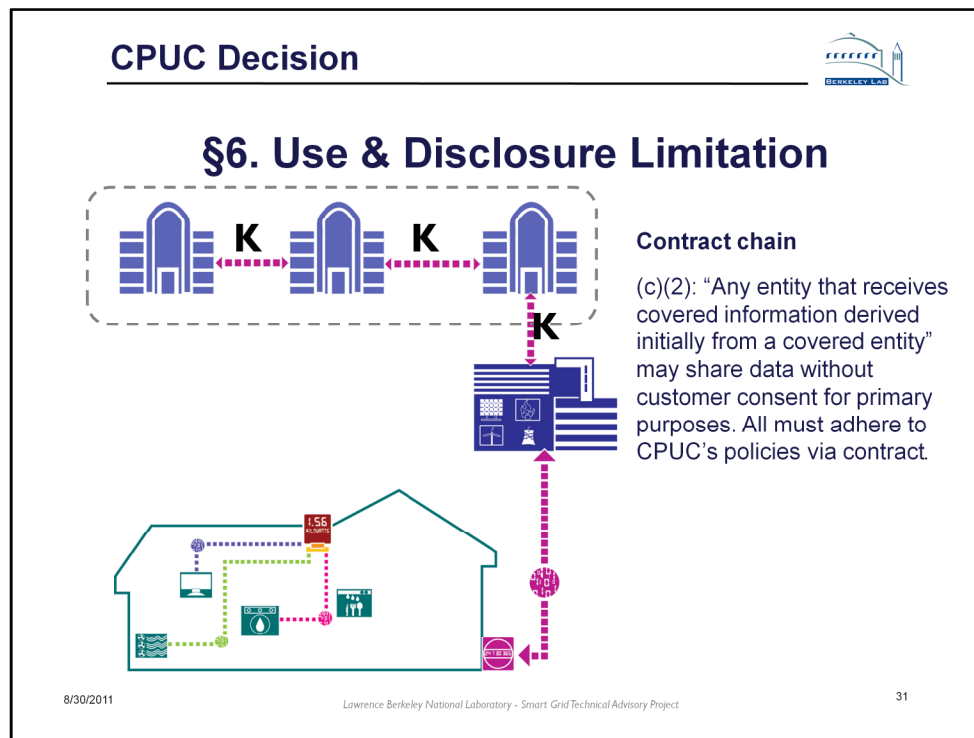
8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

30

Principle #6: Use & Disclosure Limitation.

For example,



Principle #6: Use & Disclosure Limitation.

Any entity or third-party that receives covered information from a utility is obligated to include all of the Commission rules in their contracts for services with those entities. These entities or third-parties then become subject to the same data privacy requirements as the utility. As long as this data is being used for a primary purpose, then no customer notification is required.

Under this arrangement, the utility does not include a direct liability if one of these contractual entities screws up. Although the utility is obligated to monitor their contracts and to stop providing data if a breach or other situation occurs.

Note:

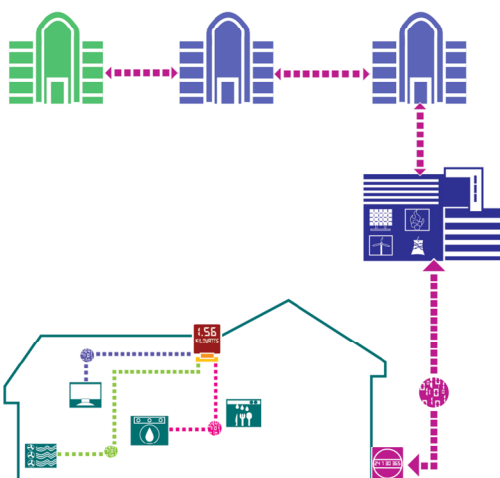
Utilities disclosing data for a primary purpose being carried out under contract with or on behalf of the utility must contractually require the third party to follow the same privacy rules the utility follows. In practice, this means that the contracted third party must follow the Commission's privacy rule.

As shown on the slide, these third parties may also employ subcontractors to fulfill some or all of their primary purpose responsibilities—therefore, the rule also requires the utility contract to require its contractor to pass along the privacy rule requirements to any subcontractor, and on down the chain.

If a party in the chain engages in a "pattern and practice" (i.e., not a one-off mistake or two) of violating the privacy rule, then the party that has been giving it data must cease. Parties who disclose data must also forward customer complaints about its contracting partners' misuse of data or other violation of the privacy rule to the Commission.

Such "chains of custody" are common data management tools.

§6. Use & Disclosure Limitation



(d): Customer consent is always required to disclose covered information for any secondary purpose.

(e): Customers can revoke authorization at any time.

8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

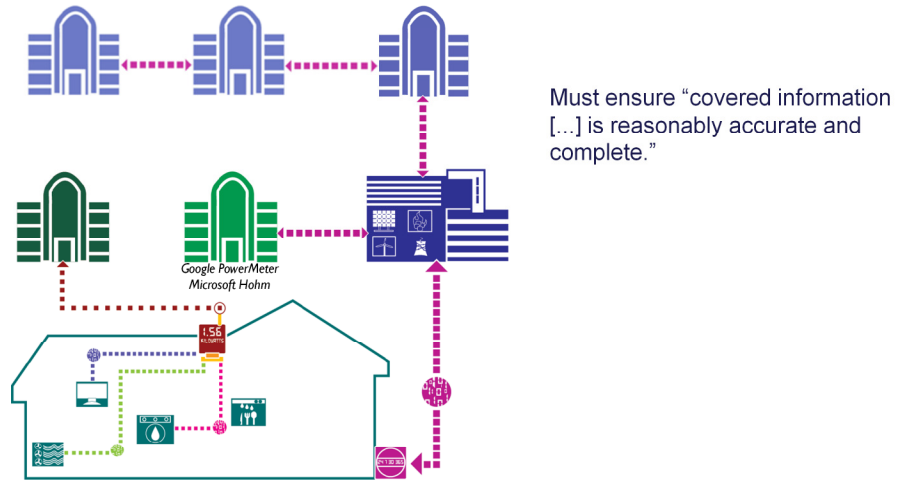
32

Principle #6: Use & Disclosure Limitation.

Customer consent is required if the data provided in this contractual arrangement for a primary purpose now begins to use the data for any secondary purpose. Under any secondary application, the customer can at any time revoke authorization for use of their data.

Update: The Proposed Decision allowed customers to opt out of data use by third parties who contract with utilities to provide energy management services (for example, OPower) (because such services are primary purpose services, the rule does not require prior consent). However, the final rule eliminated this opt-out right.

§7. Data Quality & Integrity



8/30/2011

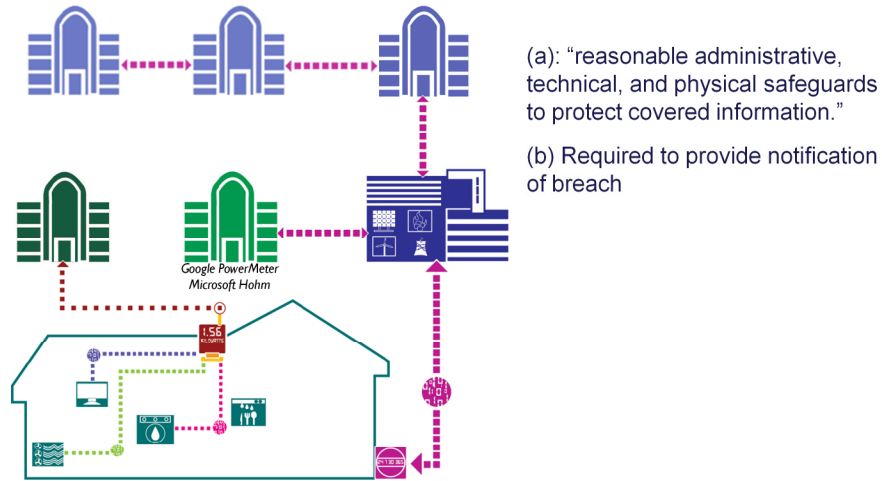
Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

33

Principle #7: Data Quality & Integrity

Under the FIPs, utilities require the data be kept reasonably accurate and complete.

§8. Data Security



8/30/2011

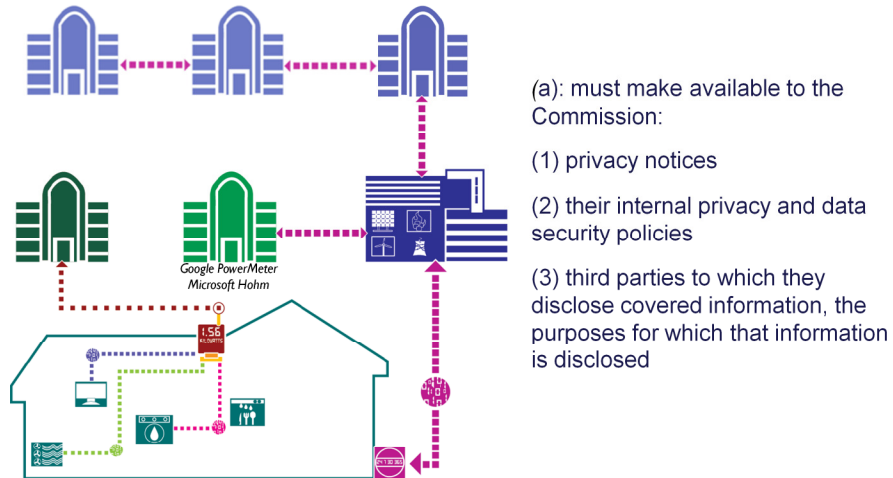
Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

34

Principle #8: Data Security

Data must be kept secure based on cyber security safe guards, which includes physical, technical, and administrative safe guards. There is also a requirement that if there is a breach in data security and information disclosed, the entity subject to the breach has to notify the customers.

§9. Accountability & Auditing



8/30/2011

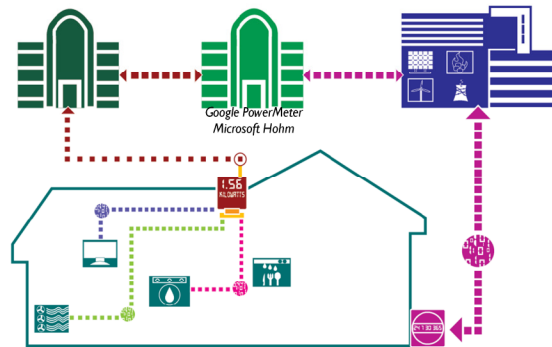
Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

35

Principle #9: Accountability & Auditing

The FIPs provides the Commission and advocates with means to determine if the rules are being followed appropriately and whether there have been breaches. To facilitate this process, the FIPs requires accountability and auditing requirements that the Commission can request.

§9. Accountability & Auditing



(d): Electrical corporations must do audits.

(e)(1): Must report "the number of authorized third parties accessing covered information."

Overarching Policy Issues



- ☐ **Privacy in the home**
- ☐ **Jurisdictional Issues**
- ☐ **Engagement with other State and Federal Actors**
- ☐ **Relationship between privacy rules and innovation**
- ☐ **Technical Implementations of DR and LC can make privacy easier or harder to address**

8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

37

Overarching Policy Issues

- Privacy in the home: How should Commissions think about privacy in the home, how the data travels, and what it is being used for.
- Jurisdictional Issues: Data generally only travels between the home and utility, however now with Smart Grid, data may now flow out of the house not under utility control and may involve many other entities not typically under Commission jurisdiction.
- Engagement with other State and Federal Actors: All of the state and Federal laws regarding data will now come into play.
- Relationship between privacy rules and innovation: This was covered only briefly. Possibilities for positive customer products and services are essential to smart grid, so privacy rules should be calibrated to preserve competition and innovation.
- Technical implementations of DR and LC can make privacy easier or harder to address: Data minimization principles might suggest that Commissions need to carefully determine what information is essential and needs to be collected versus what is unique to a particular business model.

Finally, it is unclear how and when research organizations can get access to the information necessary to advance the smart grid objectives. Commissions need to think about this issue as well.

References



	Title	Link
1	Mulligan, Deirdre K., Wang, Longhao and Burstein, Aaron J., Privacy in the Smart Grid: An Information Flow Analysis, On behalf of California Energy Commission, Public Interest Energy Research Group, March 1, 2011. Available at SSRN:	http://ssrn.com/abstract=1815605
2	P.A. Subrahmanyam, D. K. Mulligan, D. Wagner, U. Shankar, E. Jones, J. Lerner, "Network Security Architecture for Demand Response/Sensor Networks". Technical report, On behalf of California Energy Commission, Public Interest Energy Research Group, January, 2009.	<ul style="list-style-type: none"> • http://sites.energetics.com/MADRI/toolbox/pdfs/standards/network_security_final_report.pdf • http://www.law.berkeley.edu/4727.htm
3	Lerner, Jack I. and Mulligan, Deirdre K., Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home, Stanford Technology Law Review (STLR), Vol. 3, 2008. Available at SSRN:	http://ssrn.com/abstract=1099121
4	Proposed Decision Adopting Rules to Protect the Privacy and Security of Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company, in Re: Remaking 08-15-009, California Public Utilities Commission, filed May 6, 2011	http://docs.cpuc.ca.gov/EFIL/FILE/PD/134875.pdf
5	Comments of the Center for Democracy & Technology, on Draft NIST Interagency Report (NISTIR) 7828, Smart Grid Cyber Security and Requirements, National Institute of Standards and Technology, Dec. 1, 2009	http://www.cdt.org/content/cdt-comments-nist-smart-grid
6	DECISION ADOPTING RULES TO PROTECT THE PRIVACY AND SECURITY OF THE ELECTRICITY USAGE DATA OF THE CUSTOMERS OF PACIFIC GAS AND ELECTRIC COMPANY, SOUTHERN CALIFORNIA EDISON COMPANY, AND SAN DIEGO GAS & ELECTRIC COMPANY, California Public Utilities Commission, filed July 28, 2011	http://docs.cpuc.ca.gov/WORD_PDF/FINAL_DECISION/140369.pdf

Slide graphics credit: Brian P. Miller Photo & Design, <http://www.brianpmillerphotography.com/>

8/30/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

36

Contact Information



- ☐ **Chuck Goldman**
Lawrence Berkeley National Laboratory
CAGoldman@lbl.gov
510 486-4637
- ☐ **Roger Levy**
Smart Grid Technical Advisory Project
RogerL47@aol.com
916 487-0227
- ☐ **Deirdre Mulligan**
Faculty Director, Berkeley Center for Law and Technology
dkm@ischool.berkeley.edu
510-642-0499
- ☐ **Jennifer Urban**
Director, Samuelson Law, Technology & Public Policy
jurban@law.berkeley.edu
510-642-7338

8/25/2011

Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

39